IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2458

Sami Vaarala and Antti Nuopponen

Serial No. 10/500,930

Filed: 19 October 2005

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Examiner: Afshawn M. Towfighi

Date: 16 November 2010

Attorney Docket No. 290.1078USN

AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This is in response to the Office action of 26 August 2010. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising:

the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer,

sending the secure message from the first computer to the intermediate computer,

the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer,

the intermediate computer substituting the first destination address with the second destination address to the second computer,

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection ~~without establishing a new secure connection and without involving the second computer~~, and

the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique

identity.

8. (Previously presented) The method of claim 1 wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer.

11. (Previously presented) The method of claim 1 wherein the method further comprises the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer.

12. (Previously presented) The method of claim 11 wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer.

13. (Previously presented) The method of claim 12 wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer.

14. (Previously presented) The method of claim 12 wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply.

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the method further comprises defining the address so that the

first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Currently amending) A telecommunication network for secure forwarding of messages, comprising:
a first computer, a second computer and an intermediate computer,
means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point,
the first and the second computers having means for performing an IPSec processing,
the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and
the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association.

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPSec translation

has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Previously presented) The telecommunication network of claim 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

27. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:
a first computer,
a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and
the intermediate computer having means for performing translation between destination addresses and secure identities for forwarding secure messages received from the

first computer to the second computer in the secure connection.

REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested. Claims 1-2, 4-27 were rejected under Section 102 as being anticipated by Kunzinger. This rejection is respectfully traversed. No new matter has been added to the application.

Claim 1 has been amended to clarify that the first computer and second computer negotiate and exchanges key with one another to establish the secure connection. Support may be found in, for example, paragraphs 0075-0093 of the corresponding published US 2006/0173968. The secure connection extending between the first computer and the second computer is shown in Fig. 1.

Kunzinger merely teaches the use of cascaded tunnels (see abstract) in which, as shown in Fig. 4, a first tunnel extends between the first computer (client) and the intermediate computer (boundary device) and a second tunnel extends between the intermediate computer and a second computer (server). The first tunnel provides security through the Internet and the second tunnel provides security through an intranet (see paragraph 0051). Kunzinger explains in paragraph 0047 that the "use of cascaded tunnels (as opposed to a single tunnel or SA extending from the client to the server) allows security protection to be tailored to the

requirements of a particular network segment." He also explains that the security gateway serves as a point of entry into the intranet (paragraph 0050) and that the security gateway 420 retains the ability to provide of the type of services available in the environment of Fig. 3. These services include access control and network address translation that require content inspection. In other words, the gateway protects the intranet from undesirable communication from the open Internet by inspecting the content of incoming packets before the packets enter into the intranet. In paragraph 0013, Kunzinger explains that the security associations are negotiated between the tunnel endpoints i.e. between the endpoints of tunnel 1 and the endpoints of tunnel 2. This means the client 405 negotiates with the gateway 420 to establish tunnel 1 (but not with the server 440). Similarly, the gateway 420 negotiates with the server 440 to establish tunnel 2.

It is submitted that Kunzinger and the other cited references fail to teach or suggest the step of the first and second computers exchanging keys with one another to establish the secure connection that has a source address of the first computer and a destination address of the second computer.

As indicated above, Kunzinger clearly teaches the advantage of using cascade tunnels which provide the tailoring features (see paragraph 0047) "as opposed to a single tunnel or SA extending from the client to the server." Also, in

paragraphs 0012-0014 Kunzinger explains that each tunnel is a separate connection. In other words, there is no single secure connection that extends between the client 405 and the server 440 in Kunzinger's system. Also, in paragraphs 0067-0068 Kunzinger explains if there is no existing cascaded tunnel available between the gateway 420 and the server 440 then a pair of IKE and IPSsec security associations will be established to provide the next tunnel (which again indicates that there are two separate tunnels and not a single tunnel).

In view thereof, Applicants even submit that Kunzinger teaches away from the first computer and the second computer negotiating and exchanging keys with one another to establish a secure connection between the first computer and the second computer. More particularly, Kunzinger fails to teach or suggest the direct exchange of keys between the client 405 and the server 440. The key exchanges described in Kunzinger are only between the client (first computer) and the gateway (intermediate computer) to establish tunnel 1 and then between the gateway (intermediate computer) and the server (second computer) to establish tunnel 2. In other words, in Kunzinger the client 405 first exchanges keys with the gateway 420 (intermediate computer) and thereafter the gateway 420, in turn, exchanges keys with the server 440 (the second computer). There is thus no direct exchange between the client 405 and the server 440 to establish a tunnel between the client 405 to the server 440. There is therefore no key

exchange between the client and the server either.

On page 4, line 3 of the Office action, the Examiner states that "the key is the id." Applicants are puzzled over this statement. The exchange of keys is a basic concept in all kinds of cryptography to encrypt and decrypt information. In the present invention, the unique identity is in the secure message and it would not make sense to send the key together with the secure message itself. This would make the encryption meaningless since any recipient would be able to decrypt the secure message with the key. It is like locking a door but leaving the key in the door. It is therefore submitted that the key in Kunzinger does not correspond to the unique identity of the present invention.

It is submitted that Kunzinger would require extensive modifications that are not taught or suggested to arrive at the features of the present invention. Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger to learn about the single secure connection and the key exchange between the first and second computer when Kunzinger completely fails to teach or suggest these steps.

In view thereof, claim 1 is submitted to be allowable.

Claims 2, 4-21 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in

the cited references.

Independent claims 22 and 27 are submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1. More particularly, it is submitted that none of the cited references teaches means for directly exchanging and negotiating keys between the first and second computer. As explained above, an important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. There should therefore be no direct communication between the client and the server since the role of the gateway is to inspect the incoming packets before they enter the intranet.

In view thereof, claims 22 and 27 are submitted to be allowable.

Claims 23-26 are submitted to be allowable because they depend upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Claim 3 was rejected under Section 103 as being obvious over Kunzinger in view of Patel. This rejection is respectfully traversed.

Claim 3 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the

cited references.

The application is submitted to be in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1078USN

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: (910) 687-0001
Facsimile: (910) 295-2152